LAHORE UNIVERSITY OF MANAGEMENT SCIENCES

Data Handling Procedure

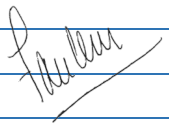
Procedure Number

Contents

DOCUMENT CHANGE RECORD

Author	Version Number	Change Reference	Signature	Date
Faizan Sarwar (Ebryx)	1.0			11 February 2023
Faizan Sarwar (Ebryx)	1.1	Cloud within Pakistan restriction removed		7 April 2023
Faizan Sarwar (Ebryx)	1.2	Updated the metadata procedure		30 May 2023
Faisal Sharif (Ebryx)	1.3	Added the Data Duplication controls.		27 October 2023

Approvals

Name	Designations	Signature	Date
Faisal Kheiri	Director IST		June 4, 2024

1. Purpose

This procedure gives the framework for handling the classified data. The users of Data at LUMS or outside LUMS are expected to responsibly manage, handle, and use institutional data. While such data may be accessed from a university-owned, personally owned, or third-party computer or device.

2. Scope

This procedure is for all employees, contractors, and third-party agents of the organization as well as any other organization affiliate who is authorized to access organizational data.

3. Definitions

a) **Data Asset (Atomic Data):** Data Asset means any data within an organization that logically cannot be further subdivided.

b) **Compound Data Asset:** Compound data assets are a type of data asset that consists of multiple atomic data assets that have been combined to create a more complex and valuable resource. These atomic data assets are any type of data and can come from a variety of sources and formats. Data users can have different views of compound Data assets according to their needs. An example of a compound data asset in a university is a dataset that combines information on a student's name, academic performance, and other information to make a student profile.

c) **Data governance management committee (DGMC**): A data governance management committee strategizes the enterprise-wide data governance program to enable different data governance dimensions and compliance.

d) **Office of Data Governance:** The office of data governance is a group that implements a data governance structure, and policies in the organization.

e) Chief data officer (CDO): Focus on implementing and developing enterprise-level data definitions and data management standards across the organization. Responsible for overseeing the office of data governance.

f) **Manager of Data Governance:** Responsible for managing and overseeing the office of data governance. Assisting and helping CDO in implementing and developing enterprise-level data definitions and data management standards across the organization.

g) **Data Steward:** A Data Steward has approval authority for decisions about data within their domain.

h) **Data Custodian**: The data custodian manages the technological environment where data resides. Custodians ensure safe custody, transport, and storage of data.

4. Applicability

This procedure applies to all electronic data as mentioned in the scope of the data governance program, including both original documents (data) and a copy of the data.

5. Data Handling

a) Introduction

Data handling is the process of ensuring that data is stored, labeled, protected, accessed,

encrypted, shared, printed, retained, archived, or disposed of safely and securely. These handling requirements apply to university data whether the data are at rest, in use, or in transit, and represent the minimum requirements for handling data in any classification. Data is classified into one of five types:

1) Unofficial Data
2) Public Data
3) Internal Data
4) Restricted Data
5) Protected Data

All the data in the university is classified as **Restricted** by default.

Please view the Data Classification procedure for details

Several data handling requirements are defined for each classification to appropriately safeguard the data in the data classification matrix.

b) Data Classification Matrix

The data classification matrix outlines the handling requirements for LUMS data throughout the following dimensions:

1) Knowledge
2) Labeling and Marking
3) Metadata
4) Data Storage
5) Security controls
6) Data Reuse
7) Data Access Controls
8) Data Transmission Controls
9) Data Retention
10) Data Relinquishing
11) Data Disposal

c) Guidelines for Handling Data

All employees and users of networked computing devices on the LUMS network are responsible for protecting the university's data. Therefore, all users should adhere to the following guidelines.

1) University staff should understand their roles and responsibilities for the data.
2) Data users should report any suspicious activity on their computers to the supervisor or IST department.
3) Data users should be mindful and careful while transmitting internal/restricted/protected data across the university.
4) Only encrypted data should be shared. If shared through email, the email should be secure, or the data and encryption key should be shared separately.
5) Internal/Restricted/Protected data should only be published in university official mediums. All restricted/protected data should be encrypted, and password protected.
6) Restricted or Protected data should only be collected with web forms that are secured via a https connection with a valid SSL certificate.
7) User computers should always be protected from viruses and other malware. Anti-virus should be on computers and set to automatically update virus definitions regularly.

8) Theft of LUMS computers should be at once reported to the IST and Office of data governance; loss or suspected compromise of internal/restricted/protected data should immediately be reported to the IST and Office of data governance.
9) Ensure the functions that enable data sharing on an individual workstation are either turned off or set to allow access only to authorized personnel.
10) Restricted file-sharing protocols should be on computers to mitigate the risk of unintentionally granting access to unknown parties.
11) Data that is categorized as restricted or protected should not be stored on a personal laptop, desktop, tablet, phone, or another end-user device.
12) Data must be stored within university premises, or on the cloud service(s) approved by the university.
13) Employee passwords should comply with the university's password guidelines.
14) Employees should not share passwords or accounts.
15) Ensure that remote access (from off-campus) connections should be done securely using HTTPS, SSH, or VPN.

6. Data Knowledge

The knowledge about the data classification is explained in section 5a.

7. Data Labeling and Marking

Data marking and labeling are essential practices for managing and organizing electronic data. Data marking and labeling make it easier to search for and retrieve data when it is needed based on the classification.

a) Data Labeling & Marking Guidelines

1) Labels should accurately reflect the classification of the data. For example, use "Protected" for the protected data, and "Internal" for the internal data.
2) Metadata fields should be used to describe the classification of the data. Where labeling is not possible.
3) Color codes should be used to help quickly identify the classification of data. For example, use red for **protected data**, blue for **restricted data**, yellow for **internal data**, and green for **public data**.
4) Data stewards should regularly review and update data labels and metadata to ensure they are accurate and current.
5) The Office of data governance should provide training and awareness to all data users who handle electronic data to ensure that they understand the importance of marking and labeling data and how to properly classify and label data.

8. Metadata

Metadata is the data that provides information about other data. It is often described as

- "Data about data", or
- "Data that explains data" or
- "Data that provides increased meaning and understanding to the University's data."

Examples of metadata include information such as the title, author, date created, date modified, file size, and file format of a document or file. Metadata is commonly used to help users locate and organize information and provide additional context about the data. It can be found in a variety of settings, including digital media, libraries, archives,

and scientific research. Metadata can be either embedded within the data itself or stored separately as a separate file or database. By effectively identifying and managing metadata, LUMS can keep data accurate, compliant, and efficient. This ensures that data is handled correctly throughout its lifecycle.
At LUMS the following guidelines should be followed for the metadata.

Guidelines

1) Data stewards will identify which data elements to store as metadata. These elements are vital for deciding and performing important data governance tasks, such as, but not limited to, when to archive data, how long to retain data, when to delete data, etc.
2) Metadata should be captured; within the systems or applications, the compound data assets are generated and managed.
3) Metadata should be automatically generated by the systems or applications for the compound data asset.
4) Metadata should be stored beside the data asset.
5) The office of data governance through its data stewards, data officers, or data custodians is responsible for the validation of metadata.

9. Data Storage

Data storage is the process of storing and preserving data for future use. It involves the physical or virtual mechanisms and technologies used to hold and retain data in various forms, such as files, databases, documents, media files, and more. Data storage is a critical aspect of data governance as it enables organizations and individuals to store, organize, access, and retrieve data efficiently and securely. Data may only be stored electronically on university owned and maintained computers and servers.

a) Cloud Data Storage

The university has a contract with different cloud services to store the data for the use of its systems for education and other purposes. This enables the university to take advantage of the features, supported systems, data storage, emails, documents, and other data related to the university.

1) Data must be on the cloud service(s) approved by the university.
2) Before any data is moved or stored in a cloud, the data owner should get approval from the data steward.

10. Data Security Controls

Security controls are measures put in place to safeguard data from unauthorized access, theft, corruption, or other malicious activities that could compromise its confidentiality, integrity, or availability.

Here are the security controls required for data at LUMS.

a) Encryption

Data encryption is the process of converting plain text or other forms of data into an unreadable format, using an encryption algorithm and a secret key. The purpose of data encryption is to protect sensitive information from unauthorized access, theft, or interception by third parties. Only those who have access to the secret key or passphrase

can decipher the encrypted data and convert it back to its original form.

b) DLP (Data Loss Prevention)

It is a security technology used to prevent the unauthorized disclosure of data, both at rest and in motion. DLP solutions use a combination of content analysis, contextual analysis, and policy-based rules to detect, monitor, and protect data from being accessed, copied, printed, transmitted, or otherwise mishandled.

c) Masking

Data masking is the process of obscuring sensitive or confidential data in a database or other data storage system, while still preserving its usefulness for testing, development, or other purposes. Data masking techniques should be used to replace data elements, such as names, addresses, ID card numbers, or credit card numbers, with fictitious or altered data that does not reveal the original values.

d) Anonymization

Data anonymization is the process of removing or modifying personally identifiable information from compound data to protect the privacy of individuals and organizations. The goal of data anonymization is to make it impossible to identify specific individuals from the compound data.

e) Backup

Data backup is the process of creating a duplicate copy of important data or information to protect it from accidental or intentional loss, corruption, or other security threats. Guidelines for data backup are given in Section 17a.

f) Guidelines for Security Controls

1) Strong encryption methods should be used to protect the data. The university should use industry-standard encryption algorithms, such as Advanced Encryption Standard (AES), to protect sensitive data.
2) University should ensure that all data transmitted between systems or devices is encrypted using secure protocols such as SSL/TLS.
3) Data storage devices such as hard drives, USB drives, and backup tapes should be encrypted.
4) Strong passwords should be used to protect encrypted data. Use strong passwords with a combination of upper and lower-case letters, numbers, and symbols.
5) Encrypted mobile devices such as laptops, tablets, and smartphones should be used to store and access data.
6) Encryption software should be regularly updated to prevent any vulnerabilities in the system.
7) Data should be monitored to detect unauthorized access or breaches. This can be done using data loss prevention tools that can monitor and control data access and usage.
8) Appropriate masking methods should be determined based on the data type being used. For example, hashing or encryption can be used for passwords, while randomization can be used for names or addresses.
9) An appropriate anonymization method based on the type of data should be determined. Common anonymization methods include randomization, suppression, and generalization.
10) All data encryption, masking, and anonymization activities should be documented including the plan and the methods used.

11.Data Sharing

Data sharing refers to the practice of distributing data assets among researchers,

students, faculty, and staff, within and outside the university for multiple purposes. The process of data sharing should be communicated and explained before sharing.

a) Guidelines for data sharing

Before sharing the data, data stewards should follow the following guideline.

1) All data sharing should be conducted with strict confidentiality in mind. Only authorized personnel should have access to sensitive data, and appropriate security measures should be in place to protect data from unauthorized access, theft, or loss.
2) Data should be shared only with individuals who have a legitimate need to know to perform their job duties or achieve specific business objectives.
3) Data should be shared only with the explicit consent of the data owner, and only for the purposes for which consent was given.
4) Data should be shared only for specific purposes, and only to the extent necessary to achieve those purposes.
5) Shared data should be accurate, complete, and up to date.
6) Shared data should be retained only for as long as necessary to achieve the purpose for which it was shared.
7) Data sharing should comply with all applicable legal and university requirements.
8) Data should be shared outside the university only after appropriate due diligence and the approval of the DGMC.
9) Data users should formally request the data from the concerned data steward. The procedure of requesting data is explained in “Requesting Data” section.

12.Data Reuse

Data reuse involves using existing data for new or additional purposes beyond its original intended use. This can include using data from one project or initiative to form another or reusing data for a different analysis or research project. The process of data reuse should be communicated and explained before sharing.

a) Guidelines for data reuse

Before sharing the data for reuse, data stewards should follow the following guidelines.

1) Data should only be reused for specific purposes that are aligned with the universities’ data governance policy, mission, and values.
2) Consent should be obtained from the data owner whose data is being reused if required by law or ethical considerations.
3) Data should be thoroughly reviewed to ensure its accuracy, completeness, and relevance for the intended reuse.
4) Before sharing data for reuse, it is crucial to categorize it and establish suitable access controls and safeguards.
5) Only authorized personnel who require access to the data should be permitted to reuse it.
6) Data should be retained only as long as necessary for the intended purpose and will be disposed of securely when no longer needed.
7) Data reuse practices should comply with all applicable laws, regulations, and university policies.
8) Data owners should be provided with clear and understandable information

about how their data is being reused.

9) Data users should formally request the reuse from the concerned data steward. The procedure of requesting data is explained in “Requesting Data” section.

13.Data Duplication

Data duplication, also called data redundancy, refers to the presence of the same data in multiple places within a database, file system, or information system. Data duplication can happen intentionally, for example, when creating backups. However, it can also happen unintentionally, for example, when users save a document to multiple folders or when two different applications store the same data in different databases.

a) Data duplication examples

Here are some examples of data duplication:

1) A user saves a copy of a file to their desktop, their laptop, and a shared drive.
2) A company stores customer data in their CRM system, their ERP system, and their marketing system.
3) A company stores backups of data in multiple locations.
4) A company stores archived data in a separate system from active data.

b) Data duplication problems

When the same information is stored or repeated in different locations, it can lead to various problems and inefficiencies. These include:

1) Increased Storage Costs: Data duplication takes up unnecessary storage space, which can be costly.
2) Performance Issues: Data duplication can slow down the performance of systems and applications, and more storage and processing power may be required.
3) Data Integrity Issues: Data duplication can compromise data integrity because it makes it difficult to maintain consistency. If one copy of the data is updated but not others, it can result in outdated, incorrect, or conflicting information.
4) Difficulty in Data Maintenance: Maintaining and updating data that is duplicated across multiple locations can be cumbersome and error prone.
5) Data Security Risks: Duplicate data increases the risk of data breaches and unauthorized access, as there are more copies that need to be secured. If one copy of the data is compromised, all the other copies are also at risk.

c) Data duplication risks mitigation

It is important to note that data duplication is not always a bad thing. In some cases, it may be necessary to have multiple copies of the same data for backup or performance reasons. However, it is important to be aware of the risks of data duplication and to take steps to mitigate them.

There are a few ways to mitigate the risks of data duplication, including:

1) Data deduplication: This is a process that identifies and removes redundant data. Deduplication can be implemented at the storage level, the application level, or both.
2) Data governance: This is a set of policies and procedures that help to ensure that data is managed consistently and accurately. Data governance policies and procedures can help to prevent data duplication from occurring in the first place.

3) Data normalization: This is a process which involves breaking down data into smaller tables and linking them through relationships in relational databases.
4) Data integration tools. These tools can help to synchronize data across multiple systems and applications. This can help to ensure that all copies of the data are up-to-date, and that duplicate data is eliminated.

d) Guidelines for data duplication

Data stewards should follow the following guidelines.

1) **Internal data**: Data to be duplicated for business purposes or in response to the request only after the authorization of data steward.
2) **Restricted data**: Employees can duplicate restricted data with the authorization of the Manager Data Governance for business or work purposes only.
3) **Protected data**: Employees can duplicate Protected data with the authorization of DGMC for business or work purpose only.
4) Data stewards should mention the roles that should have access to the duplicate data in the Data Classification Matrix against each duplicate data asset.
5) Data stewards should regularly review data duplication and in conjunction with the Office of Data Governance employ appropriate data deduplication techniques.

14.Requesting Data

Access to data should be requested in writing to the data steward from the concerned data user. **An official email account should be used to request data sharing, and the email should include a clear and detailed explanation for the request. For data reuse, the scope and purpose of reuse should be in the email.** The data stewards should comply with the request but may refer to the office of data governance if they do not consider a request valid. Similarly, the requester may report to the Office of data governance for any unreasonable delays in complying with the request.

15.Data Access Controls

Data access controls refer to a set of security measures and policies that limit and control access to internal, restricted, and protected data within LUMS. Data access controls aim to ensure that only authorized users have access to data and that data is protected from unauthorized access, theft, or misuse.

Below are the access controls required for data at LUMS:

a) Remote Access

Remote access is the ability to access data from a remote location, typically through the internet or a private network. Remote access allows users to access and work with data from outside the physical location where the data is stored.

b) Granting Access Rights

Granting access rights is the process of assigning permissions to users or groups to access specific resources or data within the university.

c) Read Access

Read access is a permission or level of access that allows a user to view or read the contents of data, but not modify or make changes to it.

d) Update Access

Update access is a permission or level of access that allows a user to modify or update the contents of data.

e) Delete Access

Delete access is a permission or level of access that allows a user to remove or delete data from a system or application.

f) Guidelines for Data Access Controls

1) A remote access policy should be developed that outlines the guidelines for remote data access, including the devices and networks allowed, the access levels, and the data to be accessed remotely.
2) Secure remote access methods such as zero-trust network access (ZTNA) and multi-factor authentication (MFA) should be used to ensure that only authorized users can access data remotely.
3) Appropriate access levels should be determined for different types of users, such as students, faculty, staff, and administrators.

16.Data Transmission Controls

Transmission controls are security measures used to protect data during transmission from one system or network to another for printing or to third parties.

a) Print Controls

Data print controls are security measures used to protect data when it is being printed or output to physical media, such as paper or disks.

b) Transmission by Public network

Data transmission from a public network is the process of sending or receiving data over a public network that is not secured. This data can be transmitted in various forms, including email messages, and file transfers.

c) Release to Third Parties

Data released to third parties is the sharing or transfer of data from a university or data used to another party who is not directly involved in the original data collection or processing. This transfer can occur for various reasons, such as business, regulatory compliance, or research purposes.

d) Guidelines for Transmission Controls

1) Printers that are used for printing internal/restricted/protected data should have limited access. This can be done by restricting access to the printer.
2) Print tracking should be implemented to monitor and control the printing of internal/restricted/protected data. This can be done using print management software that can track print jobs and monitor usage.
3) Print quotas should be enforced for users to limit the amount of printing of internal/restricted/protected data. This can help to reduce the risk of sensitive information being printed unnecessarily or without authorization.
4) Secure transmission protocols such as Secure Sockets Layer (SSL), Transport Layer Security (TLS), or zero trust network access (ZTNA) should be used to encrypt data transmitted over public networks. This helps to protect data from interception and unauthorized access.
5) Access controls should be implemented to restrict access to data transmitted over public networks to authorized personnel only.
6) Contracts that specify the terms and conditions for data release, including data security and confidentiality should be signed with third parties before releasing the data.

7) Data released to third parties should be accurate and up to date.
8) Consent should be obtained from the data owners before releasing the data to third parties.

17.Data Retention

Data should be kept for as long as it is needed to meet the operational needs of the organization, together with legal and regulatory requirements. Data should not be destroyed before the retention period has been met even though it's no longer necessary for the university.

The data retention schedule is documented in the data retention matrix.

a) Guidelines

1) Data on retention schedules will fall into two main categories.
    1) Destroy after an agreed period; where the useful life of data can be easily predetermined (for example, destroy after 5 years, destroy 2 years after the end of the fiscal year, etc.)
    2) Selected for permanent preservation; where certain groups of data can be readily defined as worthy of permanent preservation and transferred to an archive.
2) Data Retention period is for compound data assets.
3) Data retention period should depend on the nature of the data as by analyzing data, organizations can gain insights into trends and patterns, identify opportunities for improvement, and make more informed decisions.
4) The following attributes should be fulfilled for the retained data.
    - **Accurate**
      Data should always be reviewed to ensure that it is a full and correct representation of the transactions, activities, or practices.
    - **Accessible**
      Data should always be made available and accessible when needed (with additional security permissions where applicable to the document content).
    - **Complete**
      Data should have the content, context, and structure needed to allow it to continue the activities, practices, and transactions.
    - **Compliant**
      Data should always comply with any record-keeping legal and regulatory requirements.
    - **Monitored**
      The Data Retention period should be regularly monitored to ensure that the objectives and principles are always being complied with all legal and regulatory requirements.
5) Any data that is part of pending or current litigation should not be destroyed, regardless of the data retention schedule.

18.Data Archiving

Data that is no longer actively used can be archived in offline storage for long-term retention, audit, and regularity compliance purposes. The following guidelines should be considered when archiving data.

a) Guidelines

1) Data archives should be indexed and searchable so that files can be easily found and retrieved.
2) All documents stored in the archive should be protected against unauthorized access during the whole archiving process. Access to the documents should be controlled by the relevant data steward. Data within archives should be categorized and properly labeled as per the organization's data classification policy.
3) Archived data should be managed to ensure that it is unaltered, and that the original data is preserved.
4) There is always a risk of portable media (e.g., USB memory sticks, CDs, DVDs) degrading or becoming corrupted; it is therefore, the data archive should be held on a central server so that it will be effectively backed up and safeguarded from hardware failure.
5) Data held electronically should remain accessible and not become trapped in outdated technology.
6) Inbound and outbound official email messages should be archived together to meet operational needs. The retention period of emails shall be governed by the retention schedule mentioned in the organization's data retention matrix.
7) Once the archived period has elapsed, the data archives should either be reviewed, re-archived, or confidentially destroyed depending on their purpose and action type mentioned in the retention schedule.
8) Any file movement, use, or access should be tracked and logged.
9) There should be periodic reviews of the archived data.
10) Periodically restore the archived date to check the validity, accuracy, and requirement of the archived data.

19.Data Deletion

Data deletion is the process of removing or erasing data from a database or other application. This can be done manually by the user or automatically by the system. When data is deleted, it may not be immediately removed from the storage device but is usually marked as "available" space for new data to be written over software. It is important to note that deleting data does not necessarily mean that the data is gone forever, and it may still be possible for someone with the right tools and knowledge to recover it. Therefore, it is important to take appropriate measures to secure and protect sensitive data.

Here are data deletion methods:

a) Soft delete

Soft delete involves marking the data as deleted in the system's database, without physically removing the data. This method makes the record unavailable for use but still allows it to be recovered if needed.

b) Data masking

Data masking is the process of deleting sensitive data from a system, but in a way that the data can still be retrieved if needed. This is done by replacing the sensitive data with non-sensitive data, while still preserving the overall structure of the data. Data masking is a soft deletion method, as the data is still technically present in the system, but it has been obfuscated so that it is no longer sensitive. This can be a useful way to protect

sensitive data without having to permanently delete it.

c) Overwriting

This involves overwriting the data in the record with random data patterns to ensure that the original data cannot be recovered. This method can be used to delete individual records or entire databases.

To ensure that data is permanently deleted and cannot be recovered, it is recommended to use specialized data deletion tools that overwrite the data multiple times, making it nearly impossible to recover.

20. Data Disposal

Data disposal is a critical component, as it ensures that data is securely and appropriately disposed of when it is no longer needed.

a) Guidelines

The sanitization method for the media depends on the data stored on the media, the age of the media, and its next destination. Below are the terms and methods for sanitizing hard drives and other media.

a) Clearing

Clearing by overwriting is an acceptable method of scrubbing data that is not restricted or requires safeguarding. A minimum of three (3) overwrites is needed; added overwriting is recommended depending on the sensitivity of the data to be erased.

b) Purging

Purging is a form of de-magnetizing where the magnetic charge of an object is reset to a magnetically neutral state, in effect erasing all the data previously written to the hard drive or tape.

c) Destruction

In instances where the data cannot be overwritten or when degaussing is not possible, hard drives should be physically destroyed. Physical destruction is required for drives that are defective, dead, or sufficiently unresponsive that do not complete at least a three overwrite minimum.

The following table should help decide how to manage a particular computer or device.

New Location of Device	Data stored on the Device	Recommendation
Same department	No Restricted /Protected data	Clear
Another department or unit	No Restricted /Protected data	Clear
Same department to staff with access to the same data	Restricted /Protected data	Clear

Same department to staff with lower access (or student)	Restricted /Protected data	Clear
Another department or unit	Restricted /Protected data	Clear
Recycling or disposal (including surplus)	All data	Destroy
Drive manufacture date before 2001 or unknown	Restricted /Protected data	Purge
Non-functioning media	All data	Purge (magnetic); Destroy (solid state)

b) Process

1) No computers or digital storage devices should leave the university's possession without undergoing the disposal procedure.
2) Concerned data steward should advise the disposal of the data.
3) The data custodian should perform the disposal as per the above guidelines. **Note:** Data held in the university's online applications or other authorized online storage cloud should be destroyed to the extent possible by using the delete facilities provided by the cloud service provider.
4) Disposal records should be maintained, including, but not limited to, disposed of data, disposal date, and name of the responsible individual(s).

21.Backup and Recovery Procedure

Backup and recovery procedures are crucial for data governance. Any loss of data is a loss of time, money, and resources. Furthermore, the loss of data can ruthlessly affect the success of a university. An effective data backup and recovery plan is crucial to the LUMS.

a) Backup plan

1) DGMC should determine which data is critical to the functioning of the university and should be regularly backed up. This may include student and faculty records, financial data, research data, and administrative documents.
2) Data backups should be masked,-encrypted, and password protected.
3) Data backups should be performed daily by the end of the day for the critical data. Weekly backups for less critical data.
4) Two backups of all critical data should be taken on two separate mediums and two separate locations, for example,
    a. One backup on-site on a tape, or a dedicated server or network-attached storage device
    b. 2nd backup offsite, on the cloud, or remote backup service
5) The offsite location should be secure and free from environmental hazards such as floods, fires, and earthquakes. It should also be protected from theft and vandalism.
6) The offsite location should be at least 100 KM far from the primary location to

minimize the risk of both locations being affected by the same disaster. However, it should also be close enough to allow for quick retrieval of the backup media in case of a disaster.

7) Data backups should be performed and monitored by a data custodian.
8) Periodic tests should be performed to ensure that the data from the backup can be restored quickly, and that the data is complete and accurate.
9) Plans for recovering data in case of a disaster, such as a cyberattack or natural disaster, should be in place and tested. This plan should include steps for restoring data from the backup and ensuring that systems are up and running as quickly as possible. Assign roles and responsibilities to staff members who will be responsible for implementing the disaster recovery plan.
10) Ensure that all staff responsible for data management are trained in backup and recovery procedures and that they understand their roles and responsibilities in case of a disaster.
11) The last backup of every month should be considered the monthly backup. The last backup of every year should be considered annual backup and kept for three years before reusing.
12) Backup failures should be reported to the office of data governance and appropriate corrective and preventive action should be taken.
13) Backups should always be performed before upgrading or modifying a server.

b) Loss & Restoration of data

1) If data loss is discovered the Office of data governance should do an immediate investigation.
2) Once the problem is figured out and data loss is contained, the IST department should go on to restore the data from the backup.
3) The IST department should determine the lost data's time and date.
4) The IST department should figure out the appropriate backup image to restore the data from.
5) CDO or Manager of data governance should monitor the restoration of data.
6) Upon restoration, the IST department should evaluate the integrity of the restored data.
7) IST department should contact the owner of the data to complete the restoration.
8) Upon approval from the owner of the data, the restoration should be considered completed.

22.Relinquishing Data

1) Employees who leave the University due to the end of a contract or termination should surrender access to university data, whether that data exists in the university or personal assets.
2) The IST department should be responsible for ensuring that any computing assets assigned to the employee during employee clearance are sanitized before being allocated to someone else.
3) In the case where an employee has received approval to buy back a university computing asset, the IST department should ensure all university data has been removed before granting clearance approval.
4) Ex-employees are not entitled to request or keep university data, even if they were the owners of that data during their tenure.

23.Related Documents

Data Retention Matrix v1.0
Data Classification Matrix 1.0
Data Classification Procedure v1.0